REMARKS

The Examiner has rejected Claims 1, 2, 9, 34, 37-40, and 42-46 under 35 U.S.C. 101 as being directed to non-statutory subject matter. Applicant respectfully disagrees with such rejection, but asserts that such rejection is avoided in view of the amendment made to independent Claim 1 hereinabove.

The Examiner has rejected Claims 1, 2, 9, 21, 27-30, 37-39, and 42-45 under 35 U.S.C. 103(a) as being unpatentable over Khaishgi et al. (U.S. Patent No. 6,658,394), in view of Guirguis ("Network- and Host-Based Vulnerability Assessments: An Introduction to a Cost Effective and Easy to Use Strategy"), in view of Tiso ("Automated Security Scanning"), in view of Bunker, V et al. (U.S. Patent Publication No. 2003/0028803), and further in view of Blyth ("An XML-based architecture to perform data integration and data unification in vulnerability assessments"). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims.

With respect to the independent claims, the Examiner has relied on Page 16, first paragraph, as well as Figures 1 and 6 (reproduced below) from the Blyth reference to make a prior art showing of applicant's claimed technique "wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with a device record that is further in association with an account number of a provider of the online service" (as amended - see this or similar, but not necessarily identical language in the independent claims).

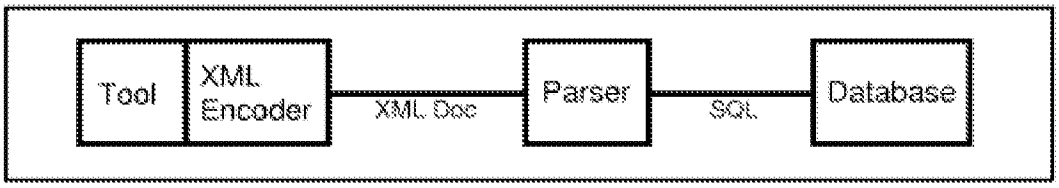

Figure 1: The general architecture.

```
  $ psxml -p 80 -v -h 10.63.19.13 | xmldb -v -c
/etc/xmldb.conf
  The PortScanning XML Tool Version 1.0 (ajoblyth@glam.ac.uk)
  Interesting ports on www.my-victim.com (10.63.19.12)
  Port              State        Service
  80                open         http
  Connecting to database xmldb on host db.my-hacker.ac.uk
  Inserting information regarding port: 80/open/http
```

Figure 6: Port scanning and database tools output.

Further, in the Office Action dated 02/19/2010, the Examiner has argued that "Fig. 6 [of Blyth] clearly discloses [that] the result of the scan includes the URL and an IP address of a provider of the online service both of which can be interpreted as an account number," that "[b]oth the URL and an IP address are registered in DNS and are used to identify the online service provider," and that "therefore both the URL and IP address can be interpreted as an account number of a provider of the online service." Furthermore, the Examiner has argued that "Fig. 2… discloses Target field in the XML and see, Fig. 5, Which discloses database containing a target field, all the vulnerabilities are stored in association with the target address which in an IP address and URL of the online service for which the scanning is performed."

Applicant respectfully disagrees and asserts that the above excerpt relied on by the Examiner merely discloses that "[t]he output from the port scanning tool, or the vulnerability scanning tool, is used to create the XML document that is then passed to the parser, which uses it to create a DOM tree," and that "[t]he parser parses the XML documents with reference to their document type definitions (DTD) to check that the XML documents are valid and well formed" (Page 16, first paragraph). In addition, the figures relied on by the Examiner merely disclose a parser, and additionally disclose "an example of the psxml and xmldb tools running in verbose mode," where "psxml is a simple port scanning tool" and where an "XML document is… passed to the back-end XML database system called xmldb" (Page 19, second paragraph).

Further, applicant notes that Figure 6 discloses "[p]ort scanning and database tools output," where, as mentioned above, the output is used to create an XML document that is passed to a parser. Additionally, Figure 4 merely illustrates a "system" database table that includes a "sysm_id" field, an "ip" field, a "target" field, and a "type" field. In addition, Figure 5 merely illustrates a "vuln" database table that includes a "vul_id" field, a "timestamp" field, a "timezone" field, a "target" field that references the system table, a "scantool" field, a "scanvsn" field, and a "state" field.

However, disclosing an output of a port scanning tool and a database tool that is used to create an XML document, where the output includes a URL and IP address, in addition to disclosing that the XML document is passed to a back-end XML database system called xmldb, where the database system includes a system table, which includes an IP address field and a target field, and a vuln table, which includes a target field that references the system table, as in Blyth, simply fails to support the Examiner's assertion that "both the URL and IP address can be interpreted as an account number of a provider of the online service," and further fails to suggest applicant's claimed technique "wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with a device record that is further in association with an account number of a provider of the online service" (emphasis added), as claimed by applicant.

Clearly, disclosing that the target field of the vuln table references the target field of the system table, which also includes an ip address field, as in Blyth, simply fails to even suggest any sort of "an **account number** of a **provider** of the online service," much less "stor[ing] records of the parsed set of XML files in the database in association with a device record that is further in association with an account number of a provider of the online service" (emphasis added), as specifically claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the

reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 42, the Examiner has relied on Paragraphs [0052] and [0054] from the Bunker reference to make a prior art showing of applicant's claimed technique "wherein the schedule is requested by the customer." Further, in the Office Action dated 02/19/2010, the Examiner has argued that "the tests for vulnerability are scheduled according to the customer profile and the customer profile is provided by the customer therefore, the schedule is requested by the customer."

Applicant respectfully disagrees and asserts that the excerpts from Bunker relied upon by the Examiner merely teach that "[t]he job scheduling module 202… uses the customer profile 204 information to tell the Command Engine 116 what services the customer should receive… so that the Command Engine 116 can conduct the appropriate range of tests 516" (Paragraph [0052] – emphasis added). Further, the excerpts teach that "[e]very customer has a customer profile 204 that may include description of the services the customer will be provided, the range of IP addresses the customer's network 1002 spans, who should receive the monthly reports, company mailing address, etc." and that "Customer Profile information includes that information discussed in this specification

which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." (Paragraph [0054] – emphasis added).

However, merely using the customer profile information to tell the Command Engine what services the customer should receive, where the customer profile information is provided by the customer and includes a description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, and a company mailing address, as in Bunker, fails to suggest applicant's claimed technique "wherein the schedule is **requested** by the customer" (emphasis added), as claimed by applicant. Clearly, a customer providing customer profile information such as IP addresses and services to be provided, as in Bunker, simply fails to even suggest that "the schedule is **requested** by the customer" (emphasis added), as specifically claimed by applicant.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 47-48 below, which are added for full consideration:

> "wherein the account number of the provider of the online service is associated with the provider's account records" (see Claim 47); and
>
> "wherein the overall numeric rating has a normalized numerical scale of 0 to 10 and is based on individual security metrics including a frequency of scan, a promptness of repair, a frequency of vulnerabilities, how recently scanned, a percentage of servers tested, and a current status" (see Claim 48).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P647).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100